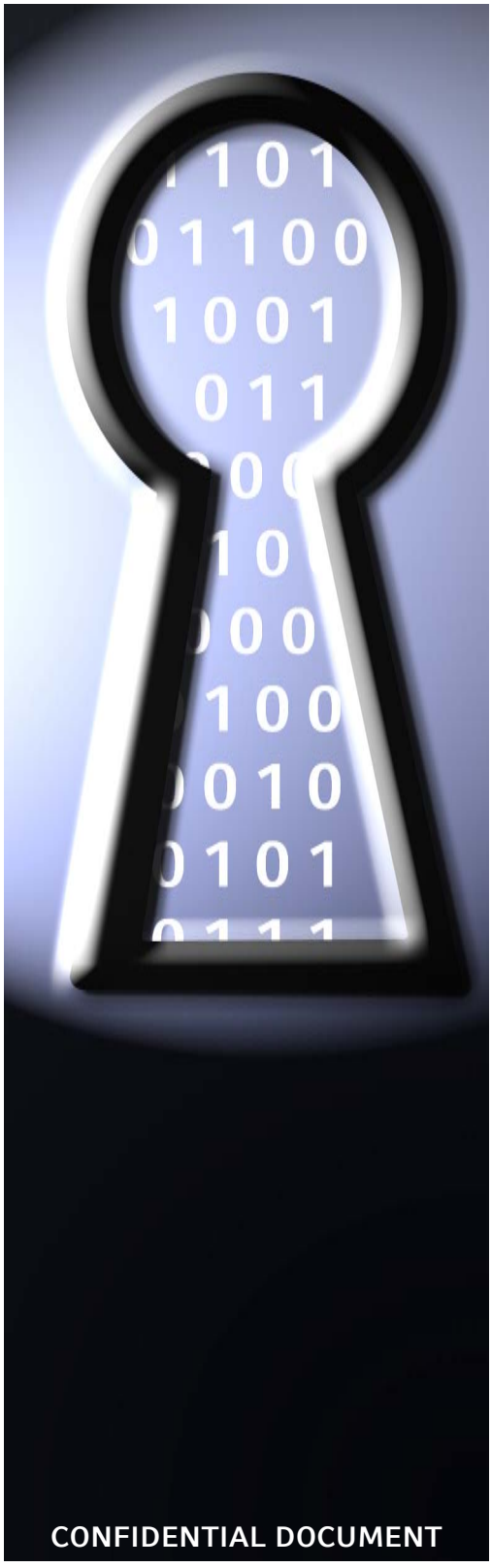
EXHIBIT H

WestLB



SECURITY AWARENESS GUIDELINES

BU IT Information Security Officer

Document Version 1.0

Contents

1. Introduction 3
2. Passwords 4
3. Safe Workstation Environment 5
4. Clear Desk/Clear Screen 6
5. Situational Awareness 7
6. Safe Data/Information Handling 8
7. Safe Use of Portable Computing Equipment 9
8. Sensible Communication Practices 10
9. Safe Disposal of Documents and Media 11
10. Recognizing Attempts at Social Engineering 12
11. Physical Security 13
12. Be Alert and Observant 14
13. Additional Responsibilities and Resources 15

1. Introduction

Business processes increasingly call for networking between the WestLB Banking Group and its customers and business partners. Opening ourselves in this way to the outside world exposes WestLB computing systems (and the information they contain) to possible misuse and compromise at the hands of hackers and others of questionable intent. This reality, in turn, introduces new demands regarding the manner in which we guarantee information security. Safeguarding this resource we call “information” requires that we all observe a number of basic rules in relation to the security of information. It is this reality that makes employee security awareness an absolute necessity.

The purpose of this Security Awareness training program is to provide all WestLB employees with the tools and concepts necessary to protect the information held by the WestLB Banking Group (hereinafter referred to as “the Bank”) from deliberate or inadvertent compromise. In this context the term *information* includes all data, programs, files and databases that are stored in computers, transmitted across networks, or printed, and also those that exist only in the form of paper. It also includes any material that is written down, or sent or received by fax, or stored on magnetic tape, diskettes or any other media, and the contents of e-mails and telephone conversations. Finally, remember that “information” also includes knowledge that exists only in your head. This information must be safeguarded as well.

All members of staff (employees, temps, consultants, etc.) are responsible for the security of the information that is entrusted to them. Within his or her area of influence, every manager is directly responsible for the implementation of and compliance with the rules governing the security of information.

In addition to the general security awareness concepts presented in this document, WestLB makes available to all employees an extensive library of Bank-specific security policies. These policies have been collected and published as local New York IT policies and globally applicable policy Manuals 130 and 101. These resources are available for review from Lotus Notes and from the local WestLB intranet site.

With this background in mind, we can now consider some security awareness concepts in detail.

2. Passwords

All members of WestLB staff have an obligation to exercise reasonable care in maintaining the security of their personal system authentication information (i.e., user IDs and passwords that allow you to access WestLB computing systems). Possession of this information is comparable to the simultaneous possession of your ATM card and its PIN. Remember, anything you are able to do on WestLB computers, someone else would be able to do if they had your password and user ID.

Password confidentiality is the **only** form of protection that prevents your personal system access accounts from being misused. User-IDs and passwords that have been given to you **are for your use only** and must not be given (or accessible) to third parties.

Here are some guidelines for ensuring the security (and confidentiality) of your passwords:

- Select a password that contains a minimum of 8 characters (or as many as the application will permit). The longer the password, the harder it is to steal or crack.
- Your password should contain a mix of letters and numbers. This serves multiple purposes. First of all, complex character strings are not easy to guess. To offer an extreme example, 2FAT4ME is more challenging to guess than TOOFATFORME would be. Second, password cracking programs used by hackers have an exponentially more difficult time of it once numbers (or special characters) are introduced into the equation.
- Your current password must differ from your prior five passwords. Using the same password repeatedly defeats the purpose of requiring password changes in the first place! The longer a given password is in use, the greater the likelihood of its being compromised.
- Passwords must not be written down. No “Post-IT” notes on the computer monitor please.
- Don’t use common words that can be easily guessed. Most password cracking programs used by hackers rely on a “brute force” dictionary search to figure out what your password is. It’s in everyone’s best interest that your password not be found in any dictionary.
- Passwords should not be the names of family members or pets nor should they be your birthday.
- Passwords must not be shared with others. Allowing someone to use your login information is like giving them the keys to your safe deposit box. If that person does something malicious, you know whose name will be associated with the evil deed, **yours**.
- Passwords must be changed at least every 60 days. Long-lived passwords have an ever-increasing probability of falling into enemy hands.
- Finally, err on the side of caution and change your password any time you think it may have been compromised.

3. Safe Workstation Environment

WestLB equips its employees with computing equipment that provides all functionality required to perform a particular job function. The programs installed on your workstation (or laptop) have been carefully selected and configured in a manner that maximizes both system stability and security. The Bank expects that you will use your computer prudently and in accordance with the Bank's published "acceptable use" policies. It is also expected that you will take appropriate precautions to ensure that others do not use your computer improperly.

Some things you should keep in mind:

- Users of WestLB computing equipment must not alter its configuration in any way. Program settings should not be changed without first consulting IT. If you think an option needs to be changed or an operational parameter needs to be adjusted or reset, don't do it yourself; call the Help Desk.
- Do not attempt to deactivate installed virus checking software. Anti-virus software is one of the Bank's primary weapons in fending off the barrage of malicious program code circulating in cyberspace.
- Do not install any programs not supplied by WestLB Systems on your computer. This includes both commercial products for which you may be licensed as well as shareware/freeware that may have been downloaded from the Internet. Even popular and seemingly innocuous programs such as "Webshots", or fancy fonts and cursors must not be installed. Non-standard software may interfere with the proper functioning of required programs, may adversely affect system performance, and (most importantly!), may contain malicious code (e.g., worms, viruses, Trojan horses, etc.) that can compromise security.
- Workstations that are to be left unattended for extended periods of time (e.g., lunch) should either be logged off or locked (<CTRL+ALT+DEL>, <ENTER> or through use of a screensaver with password). When you leave the office for the day, be sure to log yourself off. A logged on but unattended workstation is the equivalent of a "welcome mat" for unauthorized users seeking access to WestLB applications. Remember, any mischief perpetrated by such individuals while using your workstation will be traced back to **you**!
- Don't allow others to "borrow" your workstation. Make sure you're present any time someone else is using your computer. Just because they aren't logged in under your user-ID doesn't mean you're safe. Anything residing on your workstation hard drive (e.g., documents, emails, spreadsheets, etc.) may be subject to copying, alteration, or deletion.
- If WestLB has provided you with a laptop computer (instead of or in addition to a desktop/tower computer) make sure it's physically tethered in place at all times with a cable locking device. Laptop theft has reached epidemic proportions. Think of what you may stand to lose: the computer itself (of course), confidential data, documents, emails, contact lists, personal information, etc. If you weren't provided with a cable lock, put your laptop to bed in a locked cabinet or drawer; you'll both sleep better.

4. Clear Desk/Clear Screen

Don't be lulled into a false sense of security just because your computer and work area are located on WestLB premises. You still need to be concerned with prying eyes and sticky fingers. Don't automatically assume you're among friends. Employees (disgruntled or otherwise) may have their dark side and non-employees (e.g., janitorial staff, vendors, etc.) are often onsite. It is always wise to exercise care in what you leave out in public view.

Keep the following in mind:

- Workstation screens that are to be left unattended should be cleared (and locked or logged off).
- Work-related documents and/or storage media should not be left on desks or in public view. This class of material includes program listings, program output, telephone/contact lists, data printouts, spreadsheets, diskettes, CD-ROMs, emails, documentation, network diagrams, floor plans, etc.
- Desks must be cleared of such material at the end of every workday.
- Locking cabinets or desk drawers should be used if available.
- Keys to locking cabinets should not be left in accessible locations (e.g., unlocked desk drawers).

5. Situational Awareness

"Situational awareness" is a phrase much beloved by the military; pilots in particular. In essence, it defines the condition of knowing what's going on around you at all times. While, admittedly, it's more important to know if there's a MIG-29 in your rear view mirror than if someone is peering over your shoulder while you surf the 'net, the phrase is relevant and should be kept in mind. Don't have tunnel vision; look around and be aware of what's going on in your immediate surroundings.

Two quick points:

- When using WestLB computing resources (e.g., your desktop workstation or laptop), be aware of who is in the vicinity. "Shoulder surfing" (i.e., watching someone else's computer screen) is one of the primary tools in the hacker's arsenal.
- Keep your computer screen turned away from prying eyes. If this is not possible, consider relocating or deferring your work until "the coast is clear."

6. Safe Data/Information Handling

WestLB's most valuable asset (aside from you, of course) is its data and other intellectual property. It is every employee's responsibility to safeguard the integrity of this material (whether electronic or paper-based or even the WestLB-related knowledge in your head) in a manner commensurate with its importance. Remember, it's not just theft that we need to be concerned about. Valuable data or information can also be lost due to technical malfunctions such as disk drive "crashes" and also through carelessness by divulging it to the wrong audience. "But", you ask, "how am I supposed to know what's important?" The answer is that the Bank has implemented a 4-tier data classification system that ranks data/information according to its value and handling requirements. Employees should familiarize themselves with this system (which is fully documented in Manual 130, available through Lotus Notes) noting in particular the safe handling and acceptable dissemination guidelines.

General "best practices" regarding the safe handling of information include the following:

- Make certain to retrieve all documents (including emails) printed on WestLB network printers. These printers are shared devices used by many people and are often located in semi-public areas. Sensitive or confidential material can easily be read or taken if left on printers for any length of time.
- Work-related files should not be stored on local workstation hard drives. These drives are not backed up on a regular basis and may, therefore, not be recoverable should a device fail. Also, theft of the computer or just its hard drive may place sensitive or confidential information in unauthorized hands.
- Work-related files should be stored on shared network drives provided for the purpose by WestLB Systems. Such drives are backed up regularly and are less prone to theft or compromise than desktop devices.
- Important documents should be shredded prior to disposal. If your department doesn't have a shredder, it would be wise to get one.
- Apply common sense. Evaluate the value or confidentiality of information you possess and think before entrusting it to others.

7. Safe Use of Portable Computing Equipment

The use of laptop computing equipment introduces a smorgasbord of security concerns over and above those associated with desktop workstations. Whereas desktop computers are insulated (to a large degree) from most avenues of physical compromise by virtue of their being located permanently on WestLB premises, laptop computers are taken from this protective cocoon and exposed to the dangers of the outside world. Employees who have been given custody of portable computing equipment must be especially vigilant.

Consider the following:

- Laptop computers are a prime target of thieves. While the loss of the hardware is significant, the loss of the data they contain is much more so.
- Password-protect important files such as spreadsheets and Word documents.
- Discuss encrypting the entire contents of the laptop's hard drive with the Information Security Officer.
- Do not connect WestLB laptop computers to non-WestLB networks whether wired or wireless. Resist the urge to connect to the Internet through public wireless "hotspots", they're not secure.
- Along the same lines, if your laptop does have wireless capability, make sure it's turned off or disabled when not needed.
- Make sure your laptop prompts you for a user-ID and password when you first turn it on. While this won't deter a determined computer thief, it will prevent the casual snoop from seeing what's on your hard drive should the computer be left unattended.
- Do not leave WestLB-issued laptops unattended. At those times when it's inappropriate to carry the computer with you, make sure it is in a secured location (e.g., locked cabinet or hotel safe). As was mentioned earlier, whenever possible, secure your laptop with a cable locking device.

8. Sensible Communication Practices

They used to say, “the walls have ears” or “loose lips sink ships.” Originally, this was meant as a warning to be circumspect in what you say and to whom. Dire consequences may ensue if sensitive information reaches an unintended audience. While the context may have changed since these phrases were coined, the message remains equally valid (if not more so) today. The dissemination of Bank-related information must be controlled and it is every employee’s responsibility to exercise good judgment in dispensing any such information that they may possess.

At a minimum:

- Do not discuss Bank business with external third parties without prior approval.
- Be careful about the contents of emails. Think about what you’re sending and to whom before pressing the <Enter> key. Once a message is sent, you can’t get it back.
- Do not send attachments of Bank documents to non-WestLB email addresses without permission.
- Consider whether certain information might be better (i.e., more safely) conveyed verbally than via email (remember, emails can be printed and/or forwarded).
- Do not open any attachments that are sent to you via email without first verifying their origin. We know that email attachments are the primary mechanism through which computer viruses and worms enter networks. But they are also a means for installing a class of malicious programs referred to as “spyware” that can capture information as well as your keystrokes and send it off to who-knows-where.
- Do not post messages containing Bank-related information to Internet bulletin boards or user groups. You never know who might be reading these messages or how the information might be used.
- Be cognizant of your surroundings when discussing the Bank or Bank business in public places. The walls have ears. “Situational awareness”, remember?
- Think before faxing. The receiving fax machine is probably located in an area accessible to many people, not just the intended recipient. Bank information can easily be misappropriated if left sitting uncollected on a public fax machine. Also, note that faxes may be stored in the memory of the receiving fax machine. These electronic images can be printed at a later time by individuals of malicious intent.

9. Safe Disposal of Documents and Media

Care should be exercised in the disposal of business-related documents and electronic storage media. Ideally, no unneeded sensitive or confidential information should leave WestLB premises or your possession without having first been rendered unusable. Carelessly discarded documents, CD-ROMs, floppy disks, etc. can provide a wealth of information to a motivated hacker who may retrieve this material simply by sifting through your trash. Don't assume that your trashcan is the final resting place of everything tossed in it.

Some additional points to ruminate over:

- Documents that are known to contain non-public information should be shredded for disposal. The Bank provides special collection receptacles for such materials. If you aren't absolutely certain that the materials you are discarding are fit for public consumption, it's best to err on the side of caution and destroy them.
- Offsite document disposal should be done with care. Do not deposit business-related documentation or storage media (e.g., floppy discs, and CD-ROMs) in publicly accessible receptacles without first rendering them unreadable. If this is not feasible, return these materials to WestLB premises where they can be disposed of properly. A common practice among hackers (known as "dumpster diving") involves sifting through corporate trash looking for valuable information or account passwords.
- Optical media (e.g., CD-ROMs, DVDs, etc.) must be rendered unreadable prior to disposal. While it is possible to snap CDs and DVDs in half yourself, the Bank would prefer that these types of media be returned to WestLB Systems which is equipped to destroy them safely.
- Magnetic storage media (e.g., floppy disks and hard disk drives) must be cleared of all data (or rendered unreadable) prior to disposal. The WestLB Information Security Officer and IT have tools and procedures in place for ensuring that all magnetic media is "scrubbed" before being discarded, donated, or sold. Consequently, do not just toss old drives or diskettes into the trash as they might wind up in a dumpster out on the street where they are accessible to "dumpster divers."

10. Recognizing Attempts at Social Engineering

Hackers and others of malicious (or at least questionable) intent have become very adept at leveraging most everyone's trusting nature and desire to be polite and helpful. They have learned to skillfully manipulate these positive character traits and turn them to their advantage. By exploiting the fact that most of us assume individuals we're in contact with are truthful and are who they say they are, masters of the art of "social engineering" are often able to extract valuable information that can be used to access and possibly compromise important computer systems. The moral is, when someone you don't know suddenly appears and tries to be your new best friend, be suspicious until you can positively establish their identity and motives. Never volunteer Bank-related information to anyone you don't know.

Don't allow yourself to be duped. Remember the following:

- Do not divulge your user-ID or password or any other personal information to **anyone** you do not know. Not all hackers are inarticulate computer nerds; some are very adept at "social engineering", the name given to the process of coaxing confidential information out of unsuspecting target individuals.
- Be suspicious of unknown callers asking for Bank-related information regardless of their cover story. If a caller claims to be from the Help Desk, for example, ask for the person's name and telephone number and refer to the Bank's online telephone directory to verify identity. Similarly, if someone calls claiming to be an auditor and inquiring if you would mind meeting to answer a few questions, a prudent course of action would be to contact the head of the Audit Department to establish that this person is not an imposter.
- You aren't being rude and shouldn't be embarrassed by politely refusing to divulge Bank information either in person or over the telephone to **anyone** you don't know.

11. Physical Security

As stated earlier, the aim of Security Awareness is ensuring the safety and integrity of the Bank's intellectual property, its "information". In seeking to accomplish this objective, it must be borne in mind that securing Bank information is, in part, contingent upon securing the "vessel" within which it resides. Gaining unauthorized access to WestLB premises and computing equipment can result in unauthorized access to WestLB information, the very resource we are most interested in securing. Consequently, it behooves us all to pay close attention to the Bank's physical infrastructure and those who have access to it.

Here are a few obvious points to consider:

- Do not "loan" your WestLB-issued ID/access card to anyone. Remember, access card usage is recorded and inappropriate use of your card will be traced back to **you**.
- Be cautious of "tailgaters" who attempt to follow you into Bank premises without using their own access card. Individuals without proper building passes should be directed to the Bank reception area on the 25th floor.
- Do not allow your visitors to move about Bank premises unescorted.
- Unrecognized individuals seen on Bank premises should be reported to management.
- Normally locked doors found to be either unlocked or ajar should be reported to Facilities Management for further investigation.
- Obvious damage to Bank equipment should also be reported to Facilities Management.

12. Be Alert and Observant

Most of us are guilty of not absorbing what's going on around us or even noticing the unique characteristics of our personal workspace. You know that poster that's been hanging on the wall behind you for the last six years? Do you know what's on it? If you're like most people, probably not. For that matter, if someone asked you what color the carpet by your desk is, would you know? Do you ever look at the informational messages that appear on your computer monitor when you sign on in the morning? The point is, we could all be more security aware if we were just more aware in general. Be aware of what's going on around you. Be aware of your environment. Be aware of what your computer is trying to tell you. And be alert for anything out of the ordinary.

Here are a few more things to keep in mind:

- Pay attention to what appears on your computer screen every day. Anything new or unusual may be a symptom of a security incident.
- Note the displayed time of last login. If you know you didn't logon to the system at that time, notify the Bank Information Security Officer (ISO).
- Don't ignore unfamiliar messages or dialog boxes that may appear on screen. If possible, capture (ALT+PRINT SCRN) and print or write down any such messages and report them to the ISO. These may be symptoms of a virus or worm infestation.
- Unusual workstation behavior should be reported to the Help Desk. Programs that had worked without problem that now terminate abnormally may also be a symptom of a security incident.
- Note where everything is in your work area and immediate vicinity. Once you have that mental picture firmly recorded, noticing if something has been taken or moved will be that much easier.
- Data files for which you are responsible that have been deleted or altered in some way without your permission should also be reported to the Bank ISO. This might be the result of malicious activity.
- Unexpected program output should be carefully considered, as this too may be a symptom of malicious activity.

13. Additional Responsibilities and Resources

While it may sound like a cliché, security **is** everyone's responsibility. All WestLB employees are expected to make security awareness an integral part of their workday. The Bank has made available for review a wide variety of resources that explain in detail all security-related policies and best practices that employees need to be cognizant of. These resources include Lotus Notes based manuals as well as documents such as the one you're currently reading. If these do not provide all the answers, feel free to contact the Bank's Information Security Officer for additional information or clarification.

To summarize:

- In addition to understanding and abiding by the general security awareness concepts presented in this document, all employees of WestLB are expected to familiarize themselves with the Bank's detailed information security policies. These policies may be viewed in their entirety in Manuals 101 and 130, both of which are accessible through Lotus Notes and the WestLB intranet. Also available for review is an extensive set of security-related policies tailored specifically to the New York office. These may be found in Manual 410, also accessible through Lotus Notes.
- Be aware that policies presented in the manuals are **binding on all employees** and compliance is mandatory.
- Employees will be required to attest to their knowledge of and compliance with Bank policies annually.
- All questions relating to information security should be directed to the Bank's Information Security Officer.